



## Features and Functionality

---

Major releases contain new features, functionality, and enhancements. Major releases can also include deprecated features and platforms, menu and terminology changes, changed behavior, and so on.



---

**Note** These release notes list the new and deprecated features in *this* version, including any upgrade impact. If your upgrade skips versions, see [Cisco Firepower Management Center New Features by Release](#) and [Cisco Firepower Device Manager New Features by Release](#) for historical feature information and upgrade impact.

---

- [Features for Firepower Management Center Deployments, on page 1](#)
- [Features for Firepower Device Manager Deployments, on page 13](#)
- [About Deprecated FlexConfig Commands, on page 20](#)
- [Intrusion Rules and Keywords, on page 21](#)
- [How-To Walkthroughs for the FMC, on page 21](#)
- [Sharing Data with Cisco, on page 22](#)

## Features for Firepower Management Center Deployments



---

**Note** Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact.

For more information, see the [End-of-Life and End-of-Support for the Cisco Firepower User Agent](#) announcement and the [Firepower User Identity: Migrating from User Agent to Identity Services Engine](#) TechNote.

---

## New Features in FMC Version 6.5.0

Table 1:

Feature	Description
<b>Hardware and Virtual Appliances</b>	
FTD on the Firepower 1150	We introduced the Firepower 1150.
Larger instances for FTDv for Azure	Firepower Threat Defense Virtual on Microsoft Azure now supports larger instances: D4_v2 and D5_v2.
FMCv 300 for VMware	We introduced the FMCv 300, a larger Firepower Management Center Virtual for VMware. It can manage up to 300 devices, compared to 25 devices for other FMCv instances.  You can use the FMC model migration feature to switch to the FMCv 300 from a less powerful platform.
VMware vSphere/VMware ESXi 6.7 support	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.7.
<b>Firepower Threat Defense</b>	
Firepower 1010 hardware switch support	The Firepower 1010 now supports setting each Ethernet interface to be a switch port or a firewall interface.  New/modified pages: <ul style="list-style-type: none"> <li>• <b>Devices &gt; Device Management &gt; Interfaces</b></li> <li>• <b>Devices &gt; Device Management &gt; Interfaces &gt; Edit Physical Interface</b></li> <li>• <b>Devices &gt; Device Management &gt; Interfaces &gt; Add VLAN Interface</b></li> </ul> Supported platforms: Firepower 1010
Firepower 1010 PoE+ support on Ethernet 1/7 and Ethernet 1/8	The Firepower 1010 now supports Power over Ethernet+ (PoE+) on Ethernet 1/7 and Ethernet 1/8.  New/modified pages: <b>Devices &gt; Device Management &gt; Interfaces &gt; Edit Physical Interface &gt; PoE</b>  Supported platforms: Firepower 1010
Carrier-grade NAT enhancements	For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888).  New/modified pages: <b>Devices &gt; NAT &gt; add/edit FTD NAT policy &gt; add/edit NAT rule &gt; PAT Pool tab &gt; Block Allocation</b> option  Supported platforms: FTD

Feature	Description
<p>TLS crypto acceleration for multiple container instances on Firepower 4100/9300</p>	<p>TLS crypto acceleration is now supported on multiple container instances (up to 16) on a Firepower 4100/9300 chassis. Previously, you could enable TLS crypto acceleration for only <i>one</i> container instance per module/security engine.</p> <p>New instances have this feature enabled by default. However, the upgrade does <i>not</i> enable acceleration on existing instances. Instead, use the <b>create hw-crypto</b> and <b>scope hw-crypto</b> CLI commands. For more information, see the <a href="#">Cisco Firepower 4100/9300 FXOS Command Reference</a>.</p> <p>New FXOS CLI commands:</p> <ul style="list-style-type: none"> <li>• <b>create hw-crypto</b></li> <li>• <b>delete hw-crypto</b></li> <li>• <b>scope hw-crypto</b></li> <li>• <b>show hw-crypto</b></li> </ul> <p>Removed FXOS CLI commands:</p> <ul style="list-style-type: none"> <li>• <b>show hwCrypto</b> (replaced by <b>show hw-crypto</b>)</li> <li>• <b>config hwCrypto</b></li> </ul> <p>Removed FTD CLI commands:</p> <ul style="list-style-type: none"> <li>• <b>show crypto accelerator status</b></li> </ul> <p>Supported platforms: Firepower 4100/9300</p>
<p><b>Security Policies</b></p>	
<p>Access control rule filtering</p>	<p>You can now filter access control rules based on search criteria.</p> <p>New/modified pages: <b>Policies &gt; Access Control &gt; Access Control &gt; add/edit policy &gt; filter</b> button ('show only rules matching filter criteria')</p> <p>Supported platforms: FMC</p>
<p>Dispute URL category or reputation</p>	<p>You can now dispute the category or reputation of a URL.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> <li>• <b>Analysis &gt; Connection Events &gt; right-click a category or reputation &gt; Dispute</b>.</li> <li>• <b>Analysis &gt; Advanced &gt; URL &gt; search for URL &gt; Dispute</b> button</li> <li>• <b>System &gt; Integration &gt; Cloud Services &gt; Dispute</b> link</li> </ul> <p>Supported platforms: FMC</p>

Feature	Description
User control with destination-based Security Group Tags (SGT)	<p>You can now use ISE SGT tags for both source and destination matching criteria in access control rules. SGT tags are tag-to-host/network mappings obtained by ISE.</p> <p>New connection event fields:</p> <ul style="list-style-type: none"> <li>• Destination SGT (syslog: DestinationSecurityGroupTag): SGT attribute for the connection responder.</li> </ul> <p>Renamed connection event fields:</p> <ul style="list-style-type: none"> <li>• Source SGT (syslog: SourceSecurityGroupTag): SGT attribute for the connection initiator. Replaces Security Group Tag (syslog: SecurityGroup).</li> </ul> <p>New/modified pages: <b>System &gt; Integration &gt; Identity Sources &gt; Identity Services Engine &gt; Subscribe to Session Directory Topic and SXP Topic</b> options</p> <p>Supported platforms: Any</p>
Cisco Firepower User Agent Version 2.5 integration	<p>We released Version 2.5 of the Cisco Firepower User Agent, which you can integrate with Firepower Versions 6.4.0 through 6.6.x.</p> <p><b>Note</b> Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact.</p> <p>For more information, see the <a href="#">End-of-Life and End-of-Support for the Cisco Firepower User Agent</a> announcement and the <a href="#">Firepower User Identity: Migrating from User Agent to Identity Services Engine</a> TechNote.</p> <p>New/modified FMC CLI commands: <b>configure user-agent</b></p> <p>Supported platforms: FMC</p>
<b>Event Logging and Analysis</b>	

Feature	Description
Threat Intelligence Director priorities.	<p>TID blocking/monitoring observable actions now have priority over blocking/monitoring with Security Intelligence Block lists.</p> <p>If you configure the <b>Block</b> TID observable action, even if the traffic also matches a Security Intelligence Block list set to <b>Block</b>:</p> <ul style="list-style-type: none"> <li>• The Security Intelligence category in the connection event is a variant of TID Block.</li> <li>• The system generates a TID incident with an action taken of Blocked.</li> </ul> <p>If you configure the <b>Monitor</b> TID observable action, even if the traffic also matches a Security Intelligence Block list set to <b>Monitor</b>:</p> <ul style="list-style-type: none"> <li>• The Security Intelligence category in the connection event is a variant of TID Monitor</li> <li>• The system generates a TID incident with an action taken of Monitored.</li> </ul> <p>Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident.</p> <p><b>Note</b> The system still effectively handles traffic as before. Traffic that was blocked before is still blocked, and monitored traffic is still monitored. This simply changes which component gets the 'credit.' You may also see more TID incidents generated.</p> <p>For complete information on system behavior when you enable both Security Intelligence and TID, see the <i>TID-Firepower Management Center Action Prioritization</i> information in the <a href="#">Firepower Management Center Configuration Guide</a>.</p> <p>Supported platforms: FMC</p>
'Packet profile' CLI commands	<p>You can now use the FTD CLI to obtain statistics on how the device handled network traffic. That is, how many packets were fastpathed by a prefilter policy, offloaded as a large flow, fully evaluated by access control (Snort), and so on.</p> <p>New FTD CLI commands:</p> <ul style="list-style-type: none"> <li>• <b>asp packet-profile</b></li> <li>• <b>no asp packet-profile</b></li> <li>• <b>show asp packet-profile</b></li> <li>• <b>clear asp packet-profile</b></li> </ul> <p>Supported platforms: FTD</p>



Feature	Description
Additional event types for Cisco SecureX threat response	<p>Firepower can now send file and malware events to Cisco SecureX threat response, as well as high priority connection events — those related to intrusion, file, malware, and Security Intelligence events.</p> <p>Note that the FMC web interface refers to this offering as <i>Cisco Threat Response (CTR)</i>.</p> <p>New/modified pages: <b>System &gt; Integration &gt; Cloud Services</b>.</p> <p>Supported platforms: FTD (via syslog or direct integration) and Classic (via syslog) devices</p>
<b>Administration and Troubleshooting</b>	
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	<p>You can use FlexConfig to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems.</p> <p>We now allow you to include the <b>ptp</b> (interface mode) command, and the global commands <b>ptp mode e2transparent</b> and <b>ptp domain</b>, in FlexConfig objects.</p> <p>New/modified commands: <b>show ptp</b></p> <p>Supported platforms: ISA 3000 with FTD</p>
Configure more domains (multitenancy)	<p>When implementing multitenancy (segment user access to managed devices, configurations, and events), you can create up to 100 subdomains under a top-level Global domain, in two or three levels. The previous maximum was 50 domains.</p> <p>Supported platforms: FMC</p>
ISE Connection Status Monitor enhancements	<p>The ISE Connection Status Monitor health module now alerts you to issues with TrustSec SXP (SGT Exchange Protocol) subscription status.</p> <p>Supported platforms: FMC</p>
Regional clouds	<p><b>Upgrade impact.</b></p> <p>If you use the Cisco Threat Response integration, Cisco Support Diagnostics, or Cisco Success Network features, you can now select a regional cloud.</p> <p>By default, the upgrade assigns you to the US (North America) region.</p> <p>New/modified pages: <b>System &gt; Integration &gt; Cloud Services</b></p> <p>Supported platforms: FMC, FTD</p>

Feature	Description
Cisco Support Diagnostics	<p><b>Upgrade impact.</b></p> <p><i>Cisco Support Diagnostics</i> (sometimes called <i>Cisco Proactive Support</i>) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.</p> <p>During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. For more information, see <a href="#">Sharing Data with Cisco, on page 22</a>.</p> <p>In Version 6.5.0, Cisco Support Diagnostics support is limited to select platforms.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> <li>• <b>System &gt; Smart Licenses</b></li> <li>• <b>System &gt; Smart Licenses &gt; Register</b></li> </ul> <p>Supported platforms: FMC, Firepower 4100/9300, FTDv for Azure</p>
FMC model migration	<p>You can now use the backup and restore feature to migrate configurations and events between FMCs, even if they are not the same model. This makes it easier to replace FMCs due to technical or business reasons such as a growing organization, migration from a physical to a virtual implementation, hardware refresh, and so on.</p> <p>In general, you can migrate from a lower-end to a higher-end FMC, but not the reverse. Migration from KVM and Microsoft Azure is not supported. You must also unregister and reregister with Cisco Smart Software Manager (CSSM).</p> <p>For details, including supported target and destination models, see the <a href="#">Firepower Management Center Model Migration Guide</a>.</p> <p>Supported platforms: FMC</p>
<b>Security and Hardening</b>	
Secure erase for appliance components on FXOS-based FTD devices	<p>You can now use the FXOS CLI to securely erase a specified appliance component.</p> <p>New FXOS CLI commands: <b>erase secure</b></p> <p>Supported platforms: Firepower 1000/2000 and Firepower 4100/9300</p>

Feature	Description
Stricter password requirements for FMC <code>admin</code> accounts during initial setup	<p>FMC initial setup now requires that you choose a ‘strong’ password for <code>admin</code> accounts. The setup process applies this strong password to both the FMC web interface and CLI <code>admin</code> accounts.</p> <p><b>Note</b> Upgrading to Version 6.5.0+ does not force you to change weak passwords to strong passwords. With the exception of LOM users on physical FMCs (and this does include the <code>admin</code> user), you are not prohibited from choosing a new weak password. However, we do recommend that all Firepower user accounts — especially those with Admin access — have strong passwords.</p> <p>Supported platforms: FMC</p>
Concurrent user session limits	<p>You can now limit the number of users that can be logged into the FMC at the same time. You can limit concurrent sessions for users with read only roles, read/write roles, or both. Note that CLI users are limited by the read/write setting.</p> <p>New/modified pages: <b>System &gt; Configuration &gt; User Configuration &gt; Max Concurrent Sessions Allowed</b> options</p> <p>Supported platforms: FMC</p>
Authenticated NTP servers	<p>You can now configure secure communications between the FMC and NTP servers using SHA1 or MD5 symmetric key authentication. For system security, we recommend using this feature.</p> <p>New/modified pages: <b>System &gt; Configuration &gt; Time Synchronization</b></p> <p>Supported platforms: FMC</p>
<b>Usability and Performance</b>	



Feature	Description
Improved initial configuration experience	<p>On new and reimaged FMCs, a wizard replaces the previous initial setup process. If you use the GUI wizard, when initial setup completes, the FMC displays the device management page so that you can immediately begin licensing and setting up your deployment.</p> <p>The setup process also automatically schedules the following:</p> <ul style="list-style-type: none"> <li>• Software downloads. The system creates a weekly scheduled task to download (but not install) software patches and publicly available hotfixes that apply to your deployment.</li> <li>• FMC configuration-only backups. The system creates a weekly scheduled task to back up FMC configurations and store them locally.</li> <li>• GeoDB updates. The system enables weekly geolocation database updates.</li> </ul> <p>These tasks are scheduled in UTC, which means that when they occur <i>locally</i> depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time.</p> <p><b>Note</b> We <i>strongly</i> recommend you review the auto-scheduled tasks/GeoDB updates and adjust them if necessary.</p> <p>Upgraded FMCs are not affected. For details on the initial configuration wizard, see the <i>Getting Started Guide</i> for your FMC model; for details on scheduled tasks, see the <a href="#">Firepower Management Center Configuration Guide</a>.</p> <p>Supported platforms: FMC</p>
Light theme	<p><b>Beta.</b></p> <p>The FMC web interface defaults to the Classic theme, but you can also choose a new Light theme.</p> <p><b>Note</b> The Light theme is a Beta feature. You may see misaligned text or other UI elements. In some cases, you may also experience slower-than-normal response times. If you encounter issues that prevent you from using a page or feature, switch back to the Classic theme. Although we cannot respond to everybody, we also welcome feedback — please use the feedback link on the User Preferences page or contact us at <a href="mailto:fmc-light-theme-feedback@cisco.com">fmc-light-theme-feedback@cisco.com</a>&gt;.</p> <p>New/modified pages: <b>User Preferences</b>, from the drop-down list under your username</p> <p>Supported platforms: FMC</p>

Feature	Description
Usability enhancements for viewing objects	<p>We have enhanced 'view object' capabilities for network, port, VLAN, and URL objects, as follows:</p> <ul style="list-style-type: none"> <li>• In the access control policy and while configuring FTD routing, you can right-click an object and choose <b>View Objects</b> to display details about that object.</li> <li>• When you are viewing details about an object, or when you are browsing objects in the object manager, clicking <b>Find Usage</b> () now allows you to drill down into object groups and nested objects.</li> </ul> <p>New/modified pages:</p> <ul style="list-style-type: none"> <li>• <b>Objects &gt; Object Management</b> &gt; choose a supported object type &gt; <b>Find Usage</b> ()</li> <li>• <b>Policies &gt; Access Control &gt; Access Control</b> &gt; create or edit policy &gt; create or edit rule &gt; choose a supported condition type &gt; right-click an object &gt; <b>View Objects</b></li> <li>• <b>Devices &gt; Device Management</b> &gt; edit FTD device &gt; <b>Routing</b> &gt; right-click a supported object &gt; <b>View Objects</b></li> </ul> <p>Supported platforms: FMC</p>
Usability enhancements for deploying configuration changes	<p>We streamlined the display of errors and warnings related to deploying configuration changes. Instead of an immediate verbose view, you can now <b>Click to view all details</b> to see more information about a particular error or warning.</p> <p>New/modified pages: <b>Errors and Warnings for Requested Deployment</b> dialog box</p> <p>Supported platforms: FMC</p>
Usability enhancements to FTD NAT policy management	<p>When configuring FTD NAT, you can now:</p> <ul style="list-style-type: none"> <li>• View warnings and errors in your NAT policy, by device. Warnings and errors mark configurations that could adversely affect traffic flow or prevent the policy from deploying.</li> <li>• Display up to 1000 NAT rules per page. The default is 100.</li> </ul> <p>New/modified pages: <b>Devices &gt; NAT</b> &gt; create or edit FTD NAT policy &gt; <b>Show Warnings</b> and <b>Rules Per Page</b> options</p> <p>Supported platforms: FTD</p>
<b>Firepower Management Center REST API</b>	

Feature	Description
New REST API capabilities	<p>Added the following REST API objects to support Version 6.5.0 features:</p> <ul style="list-style-type: none"> <li>• cloudregions: Regional clouds</li> </ul> <p>Added the following REST API objects to support older features:</p> <ul style="list-style-type: none"> <li>• categories: Categories for access control rules</li> <li>• domain, inheritancesettings: Domains and policy inheritance</li> <li>• prefilterpolicies, prefilterrules, tunneltags: Prefilter policies</li> <li>• vlaninterfaces: VLAN interfaces</li> </ul> <p>Supported platforms: FMC</p>

## Deprecated Features in FMC Version 6.5.0

Table 2:

Feature	Upgrade Impact	Description
Ability to disable the Firepower Management Center CLI	None.	<p>Version 6.3.0 introduced the Firepower Management Center CLI, which you had to explicitly enable. In Version 6.5.0, the CLI is automatically enabled, for both new and upgraded deployments. If you want to access the Linux shell (also called <i>expert mode</i>), you must log in to the CLI and then use the <b>expert</b> command.</p> <p><b>Caution</b> We recommend you do not access Firepower appliances using the shell, unless directed by Cisco TAC.</p> <p>Deprecated options: <b>System &gt; Configuration &gt; Console Configuration &gt; Enable CLI access</b> check box</p>
MD5 authentication algorithm and DES encryption for SNMPv3 users (deprecated)	None, but you should switch now.	<p>Version 6.5.0 deprecates the MD5 authentication algorithm and DES encryption for SNMPv3 users on Firepower Threat Defense.</p> <p>Although these configurations continue to work post-upgrade, the system displays a warning when you deploy. And, you cannot create new users or edit existing users with these options.</p> <p>Support will be removed in a future release. If you are still using these options in your platform settings policy, we recommend you switch to stronger options now.</p> <p>New/modified screens: <b>Devices &gt; Platform Settings &gt; SNMP &gt; Users</b></p>

Feature	Upgrade Impact	Description
TLS 1.0 & 1.1	Client may fail to connect with an upgraded appliance.	<p>To enhance security:</p> <ul style="list-style-type: none"> <li>• Captive portal (active authentication) has removed support for TLS 1.0.</li> <li>• Host input has removed support for TLS 1.0 and TLS 1.1.</li> </ul> <p>If your client fails to connect with a Firepower appliance, we recommend you upgrade your client to support TLS 1.2.</p>
TLS crypto acceleration FXOS CLI commands for Firepower 4100/9300	None.	<p>As part of allowing TLS crypto acceleration for multiple container instances on Firepower 4100/9300, we removed the following FXOS CLI commands:</p> <ul style="list-style-type: none"> <li>• <b>show hwCrypto</b></li> <li>• <b>config hwCrypto</b></li> </ul> <p>And this FTD CLI command:</p> <ul style="list-style-type: none"> <li>• <b>show crypto accelerator status</b></li> </ul> <p>For information on their replacements, see the new feature documentation.</p>
Cisco Security Packet Analyzer integration	None, but integration is no longer supported.	<p>Version 6.5.0 ends support for Firepower Management Center integration with Cisco Security Packet Analyzer.</p> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> <li>• <b>System &gt; Integration &gt; Packet Analyzer</b></li> <li>• <b>Analysis &gt; Advanced &gt; Packet Analyzer Queries</b></li> <li>• <b>Query Packet Analyzer</b> when right-clicking on an event in the dashboard or event viewer</li> </ul>
Default HTTPS server certificates	None.	<p>If you are upgrading from Version 6.4.0.9+, the <i>default</i> HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.6.0+.</p> <p>Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows:</p> <ul style="list-style-type: none"> <li>• 6.4.0.9 and later patches: 800 days</li> <li>• 6.4.0 to 6.4.0.8: 3 years</li> <li>• 6.3.0 and all patches: 3 years</li> <li>• 6.2.3: 20 years</li> </ul>

Feature	Upgrade Impact	Description
Firepower Management Center models FMC 750, 1500, 3500	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower Management Center software on the FMC 750, FMC 1500, and FMC 3500. You cannot manage Version 6.5.0+ devices with these Firepower Management Centers.
ASA 5515-X and ASA 5585-X series devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5515-X and ASA 5585-X series devices (SSP-10, -20, -40, and -60).
Firepower 7000/8000 series devices	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software on Firepower 7000/8000 series devices, including AMP models.

## Features for Firepower Device Manager Deployments

### New Features in FDM Version 6.5.0


Feature	Description
FDM support for the Firepower 4100/9300.	You can now use FDM to configure FTD on the Firepower 4100/9300. Only native instances are supported; container instances are not supported.
FDM support for FTDv for the Microsoft Azure Cloud.	You can configure on FTDv for the Microsoft Azure Cloud using FDM.
Support for the Firepower 1150.	We introduced the FTD for the Firepower 1150.
Firepower 1010 hardware switch support, PoE+ support.	The Firepower 1010 supports setting each Ethernet interface to be a switch port or a regular firewall interface. Assign each switch port to a VLAN interface. The Firepower 1010 also supports Power over Ethernet+ (PoE+) on Ethernet1/7 and Ethernet 1/8.  The default configuration now sets Ethernet1/1 as outside, and Ethernet1/2 through 1/8 as switch ports on the inside VLAN1 interface. Upgrading to version 6.5 retains the existing interface configuration.
Interface scan and replace.	An interface scan detects any added, removed, or restored interfaces on the chassis. You can also replace an old interface with a new interface in the configuration, making interface changes seamless.
Improved interfaces display.	The <b>Device &gt; Interfaces</b> page has been reorganized. There are now separate tabs for physical interfaces, bridge groups, EtherChannels, and VLANs. For any given device model, only those tabs relevant for the model are shown. For example, the VLANs tab is available on the Firepower 1010 model only. In addition, the lists provide more detailed information about the configuration and usage of each interface.

Feature	Description
ISA 3000 new default configuration.	<p>The ISA 3000 default configuration has changed so that:</p> <ul style="list-style-type: none"> <li>• All interfaces are bridge group members in BV11, which is unnamed so it does not participate in routing</li> <li>• GigabitEthernet1/1 and 1/3 are outside interfaces, and GigabitEthernet1/2 and 1/4 are inside interfaces</li> <li>• Hardware bypass is enabled for each inside/outside pair, when available</li> <li>• All traffic is allowed from inside to outside, and outside to inside</li> </ul> <p>Upgrading to version 6.5 retains the existing interface configuration.</p>
Support ends for the ASA 5515-X. The last supported release is FTD 6.4.	You cannot install FTD 6.5 on an ASA 5515-X. The last supported release for the ASA 5515-X is FTD 6.4.
Support for Common Industrial Protocol (CIP) and Modbus application filtering in access control rules on Cisco ISA 3000 devices.	<p>You can enable the Common Industrial Protocol (CIP) and Modbus preprocessors on Cisco ISA 3000 devices, and filter on CIP and Modbus applications in access control rules. All CIP application names start with “CIP,” such as CIP Write. There is only one application for Modbus.</p> <p>To enable the preprocessors, you must go into expert mode in a CLI session (SSH or Console) and issue the <b>sudo /usr/local/sf/bin/enable_scada.sh {cip   modbus   both}</b> command. You must issue this command after every deployment, as deployment turns off the preprocessors.</p>
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	<p>You can use FlexConfig to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems.</p> <p>We now allow you to include the <b>ptp</b> and <b>igmp</b> (interface mode) commands, and the global commands <b>ptp mode e2transparent</b> and <b>ptp domain</b>, in FlexConfig objects. We also added the <b>show ptp</b> command to the FTD CLI.</p>
EtherChannel (port channel) interfaces.	<p>You can configure EtherChannel interfaces, which are also known as port channels.</p> <p><b>Note</b> You can only add EtherChannels in FDM to the Firepower 1000 and 2100 series. The Firepower 4100/9300 supports EtherChannels, but you must perform all hardware configuration of EtherChannels in FXOS on the chassis. Firepower 4100/9300 EtherChannels appear in the FDM <b>Interfaces</b> page alongside single physical interfaces.</p> <p>We updated the <b>Device &gt; Interfaces</b> page to allow the creation of EtherChannels.</p>

Feature	Description
Ability to reboot and shut down the system from FDM.	You can now reboot or shut down the system from the new <b>Reboot/Shutdown</b> system settings page. Previously, you needed to issue the <b>reboot</b> and <b>shutdown</b> commands through the CLI Console in FDM or from an SSH or console session. You must have Administrator privileges to use these commands.
Support for the <b>failover</b> command in the FDM CLI Console.	You can now issue the <b>failover</b> command in the FDM CLI Console.
Service Level Agreement (SLA) Monitor for static routes.	Configure Service Level Agreement (SLA) Monitor objects for use with static routes. By using an SLA monitor, you can track the health of a static route and automatically replace a failed route with a new one. We added <b>SLA Monitors</b> to the <b>Objects</b> page, and updated static routes so you can select the SLA Monitor object.
Routing changes in Smart CLI and the FTD API.	<p>This release includes some changes to routing configuration in Smart CLI and the FTD API. In previous releases, there was a single Smart CLI template for BGP. Now, there are separate templates for BGP (the routing process configuration) and BGP General Settings (global settings).</p> <p>In the FTD API, the paths for all methods have changed, with “/virtualrouters” inserted in the paths, with the exception of the new BGP general settings methods.</p> <ul style="list-style-type: none"> <li>• The path for static route methods was <code>/devices/default/routing/{parentId}/staticrouteentries</code>, and it is now <code>/devices/default/routing/virtualrouters/default/staticrouteentries</code>.</li> <li>• BGP methods were split into two new paths: <code>/devices/default/routing/bgpgeneralsettings</code> and <code>/devices/default/routing/virtualrouters/default/bgp</code>.</li> <li>• OSPF paths are now <code>/devices/default/routing/virtualrouters/default/ospf</code> and <code>/devices/default/routing/virtualrouters/default/ospfinterfacesettings</code>.</li> </ul> <p>If you are using the FTD API to configure any routing process, please examine your calls and correct as necessary.</p>

Feature	Description
New URL category and reputation database.	<p>The system uses a different URL database, from Cisco Talos. The new database has some differences in URL categories. Upon upgrade, if any access control or SSL decryption rules use categories that no longer exist, the system will replace the category with an appropriate new category. To make the change effective, deploy the configuration after upgrade. The pending changes dialog will show details about the category changes. You might want to examine your URL filtering policies to verify that they continue to provide the desired results.</p> <p>We also added a URL lookup feature to the URL tabs in the access control and SSL decryption policies, and on the <b>Device &gt; System Settings &gt; URL Filtering Preferences</b> page. You can use this feature to check which category a particular URL is assigned to. If you disagree, there is also a link to submit a category dispute. Both of these features take you to an external web site, which will provide detailed information about the URL.</p>
Security Intelligence uses the IP address reputation for URL requests that use IP addresses instead of hostnames.	<p>If an HTTP/HTTPS request is to a URL that uses an IP address instead of a hostname, the system looks up the IP address reputation in the network address lists. You do not need to duplicate IP addresses in the network and URL lists. This makes it harder for end users to use proxies to avoid Security Intelligence reputation blocking.</p>
Support for sending connection and high-priority intrusion, file, and malware events to the Cisco Cloud.	<p>You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, the device will send connection and high-priority intrusion, file, and malware events to the Cisco cloud.</p> <p>We renamed the Cisco Threat Response item on <b>Device &gt; System Settings &gt; Cloud Services</b> to “Send Events to the Cisco Cloud.”</p>
Cisco Cloud Services region support.	<p>You are now asked to select the Cisco Cloud Services region when you register with smart licensing. This region is used for Cisco Defense Orchestrator, Cisco Threat Response, Cisco Success Network, and any cloud feature that goes through the Cisco Cloud. If you upgrade a registered device from a previous release, you are automatically assigned to the US Region; you must unregister from Smart Licensing, then reregister and select a new region, if you need to change regions.</p> <p>We added a step to the license registration process on the Smart License page and in the initial device setup wizard. You can also see the region on the <b>Device &gt; System Settings &gt; Cloud Services</b> page.</p>



Feature	Description
FTD REST API version 4 (v4).	<p>The FTD REST API for software version 6.5 has been incremented to version 4. You must replace v1/v2/v3 in the API URLs with v4. The v4 API includes many new resources that cover all features added in software version 6.5. Please re-evaluate all existing calls, as changes might have been made to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (  ) and choose <b>API Explorer</b>.</p>
<p>FTD API support for TrustSec security groups as matching criteria for source and destination in access control rules.</p>	<p>You can use the FTD API to configure access control policy rules that use TrustSec security groups for source or destination traffic matching criteria. The system downloads the list of security group tags (SGTs) from ISE. You can configure the system to listen for SXP updates to obtain static SGT-to-IP address mappings.</p> <p>You can view the list of downloaded tags using the GET /object/securitygrouptag method, and create dynamic objects for one or more tags using the SGTDynamicObject resource. It is the dynamic objects that you can use in access control rules to define traffic matching criteria based on source or destination security group.</p> <p>Note that any changes you make to the ISE object or access control rules related to security group are preserved if you edit those objects in FDM. However, you cannot see the security group criteria in an access rule if you edit the rule in FDM. If you configure security-group-based access rules using the API, please be careful when subsequently editing rules in the access control policy using FDM.</p> <p>We added or modified the following FTD API resources: AccessRule (sourceDynamicObjects and destinationDynamicObjects attributes), IdentityServicesEngine (subscribeToSessionDirectoryTopic and subscribeToSxpTopic attributes), SecurityGroupTag, SGTDynamicObject.</p> <p>We added source and destination security group tag and name as columns in Event Viewer.</p>
<p>Configuration import/export using the FTD API.</p>	<p>You can use the FTD API to export the device configuration and to import a configuration file. You can edit the configuration file to change values, such as the IP addresses assigned to interfaces. Thus, you can use import/export to create a template for new devices, so that you can quickly apply a baseline configuration and get new devices online more quickly. You can also use import/export to restore a configuration after you reimage a device. Or you can simply use it to distribute a set of network objects or other items to a group of devices.</p> <p>We added the ConfigurationImportExport resources and methods (/action/configexport, /jobs/configexportstatus, /action/downloadconfigfile, /action/uploadconfigfile, /action/configfiles, /action/configimport, /jobs/configimportstatus).</p>

Feature	Description
Creation and selection of custom file policies.	<p>You can use the FTD API to create custom file policies, and then select these policies on access control rules using FDM.</p> <p>We added the following FTD API FileAndMalwarePolicies resources: filepolicies, filetype, filetypecategories, ampcloudconfig, ampserver, and ampcloudconnections.</p> <p>We also removed two pre-defined policies, “Block Office Document and PDF Upload, Block Malware Others” and “Block Office Documents Upload, Block Malware Others.” If you are using these policies, during upgrade they are converted to user-defined policies so that you can edit them.</p>
Security Intelligence DNS policy configuration using the FTD API.	<p>You can configure the Security Intelligence DNS policy using the FTD API. This policy does not appear in FDM.</p> <p>We added the following SecurityIntelligence resources: domainnamefeeds, domainnamegroups, domainnamefeedcategories, securityintelligencednspolicies.</p>
Remote access VPN two-factor authentication using Duo LDAP.	<p>You can configure Duo LDAP as the second authentication source for a remote access VPN connection profile to provide two-factor authentication using Duo passcode, push notification, or phone call. Although you must use the FTD API to create the Duo LDAP identity source object, you can use FDM to select that object as the authentication source for the RA VPN connection profile.</p> <p>We added the duoldapidentitysources resource and methods to the FTD API.</p>
FTD API support for LDAP attribute maps used in authorizing remote access VPN connections.	<p>You can augment LDAP authorization for remote access VPN using custom LDAP attribute maps. An LDAP attribute map equates customer-specific LDAP attribute names and values with Cisco attribute names and values. You can use these mappings to assign group policies to users based on LDAP attribute values. You can configure these maps using the FTD API only; you cannot configure them using FDM. However, if you set these options using the API, you can subsequently edit the Active Directory identity source in FDM and your settings are preserved.</p> <p>We added or modified the following FTD API object models: LdapAttributeMap, LdapAttributeMapping, LdapAttributeToGroupPolicyMapping, LDAPRealm, LdapToCiscoValueMapping, LdapToGroupPolicyValueMapping, RadiusIdentitySource.</p>

Feature	Description
FTD API support for site-to-site VPN connection reverse route injection and security association (SA) lifetime.	<p>You can use the FTD API to enable reverse route injection for a site-to-site VPN connection. Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. By default, static RRI, where routes are added when you configure the connection is enabled. Dynamic RRI, where routes are inserted only when the security association (SA) is established, and then are deleted when the SA is torn down, is disabled. Note that dynamic RRI is supported for IKEv2 connections only.</p> <p>You can also set the security association (SA) lifetime (in seconds or in kilobytes transmitted) for the connection. You can also set an unlimited lifetime. The default lifetimes are 28,800 seconds (eight hours) and 4,608,000 kilobytes (10 megabytes per second for one hour). When the lifetime is reached, the endpoints negotiate a new security association and secret key.</p> <p>You cannot configure these features using FDM. However, if you set these options using the API, you can subsequently edit the connection profile in FDM and your settings are preserved.</p> <p>We added the following attributes to the SToSConnectionProfile resource: dynamicRRIEEnabled, ipsecLifetimeInSeconds, ipsecLifetimeInKiloBytes, ipsecLifetimeUnlimited, rriEnabled.</p>
Support for Diffie-Hellman groups 14, 15, and 16 in IKE policies.	You can now configure IKEv1 policies to use DH group 14, and IKEv2 policies to use DH groups 14, 15, and 16. If you are using IKEv1, please upgrade all your policies to DH group 14, as groups 2 and 5 will be removed in a future release. In addition, you should avoid using DH group 24 in IKEv2 policies, and MD5 in any IKE version, as these will also be removed in a future release.
Performance improvements when deploying changes.	<p>If you add, edit, or delete access control rules, the system has been enhanced to deploy your changes more quickly than was done in previous releases.</p> <p>For systems configured in a high availability group for failover, the process for synchronizing the deployed changes to the standby device has been improved so that the synchronization completes more quickly.</p>
Improved CPU and memory usage calculations on the System dashboard.	The method for calculating CPU and memory usage has been improved so that the information shown on the System dashboard more accurately reflects the actual state of the device.
When upgrading to FTD 6.5, historical report data is no longer available.	When you upgrade an existing system to FTD 6.5, historical report data will not be available due to a database schema change. Thus, you will not see usage data in the dashboards for times prior to the upgrade.

## Deprecated Features in FDM Version 6.5.0

Table 3:

Feature	Upgrade Impact	Description
Default HTTPS server certificates	None.	<p>If you are upgrading from Version 6.4.0.9+, the <i>default</i> HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.6.0+.</p> <p>Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows:</p> <ul style="list-style-type: none"> <li>• 6.4.0.9 and later patches: 800 days</li> <li>• 6.4.0 to 6.4.0.8: 3 years</li> <li>• 6.3.0 and all patches: 3 years</li> <li>• 6.2.3: 20 years</li> </ul>
Manually uploading VDB, GeoDB, and SRU updates	None, but feature is deprecated until you upgrade to Version 6.6.0+.	<p>Version 6.5.0 does not support manually uploading VDB, GeoDB, and SRU updates to the device.</p> <p>This feature <i>is</i> supported in Version 6.4.0.10 and later patches, and in Version 6.6.0+. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6.0+, without using Version 6.5.0 as an intermediate version.</p>
Universal Permanent License Reservation (PLR) mode	None, but feature is deprecated until you upgrade to Version 6.6.0+.	<p>Version 6.5.0 does not support Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with Cisco Smart Software Manager (CSSM).</p> <p>This feature <i>is</i> supported in Version 6.4.0.10 and later patches, and in Version 6.6.0+. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6.0+, without using Version 6.5.0 as an intermediate version.</p>
ASA 5515-X with Firepower Threat Defense	Upgrade prohibited.	You cannot upgrade to or freshly install Firepower Threat Defense Version 6.5.0+ on ASA 5515-X devices.

## About Deprecated FlexConfig Commands

This document lists any deprecated FlexConfig objects and commands along with the other deprecated features. For a full list of prohibited commands, including those prohibited when FlexConfig was introduced, see your configuration guide.



### Caution

In most cases, your existing FlexConfig configurations continue to work post-upgrade and you can still deploy. However, in some cases, using deprecated commands can cause deployment issues.

### About FlexConfig

Some Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2.0 (FMC deployments) or Version 6.2.3 (FDM deployments), you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

Upgrades to FTD can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can deprecate FlexConfig commands that you are currently using; your configurations are *not* automatically converted. After the upgrade, you cannot assign or create FlexConfig objects using the newly deprecated commands.

After the upgrade, examine your FlexConfig policies and objects. If any contain commands that are now deprecated, messages indicate the problem. We recommend you redo your configuration. When you are satisfied with the new configuration, you can delete the problematic FlexConfig objects or commands.

## Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs) provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU.

After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

Supported keywords depend on your Snort version:

- FMC: Choose **Help > About**.
- FTD with FDM: Use the **show summary** CLI command.
- ASA FirePOWER with ASDM: Choose **ASA FirePOWER Configuration > System Information**.

You can also find your Snort version in the *Bundled Components* section of the [Cisco Firepower Compatibility Guide](#).

The Snort release notes contain details on new keywords. You can read the release notes on the Snort download page: <https://www.snort.org/downloads>.

## How-To Walkthroughs for the FMC

FMC walkthroughs (also called *how-tos*) guide you through a variety of basic tasks such as device setup and policy configuration. Just click **How To** at the bottom of the browser window, choose a walkthrough, and follow the step-by-step instructions.



---

**Note** FMC walkthroughs are tested on the Firefox and Chrome browsers. If you encounter issues with a different browser, we ask that you switch to Firefox or Chrome. If you continue to encounter issues, contact Cisco TAC.

---

The following table lists some common problems and solutions. To end a walkthrough at any time, click the **x** in the upper right corner.

**Table 4: Troubleshooting Walkthroughs**

<b>Problem</b>	<b>Solution</b>
Cannot find the <b>How To</b> link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select <b>User Preferences</b> then click <b>How-To Settings</b> .
Walkthrough appears when you do not expect it.	If a walkthrough appears when you do not expect it, end the walkthrough.
Walkthrough disappears or quits suddenly.	<p>If a walkthrough disappears:</p> <ul style="list-style-type: none"> <li>• Move your pointer.</li> </ul> <p>Sometimes the FMC stops displaying an in-progress walkthrough. For example, pointing to a different top-level menu can make this happen.</p> <ul style="list-style-type: none"> <li>• Navigate to a different page and try again.</li> </ul> <p>If moving your pointer does not work, the walkthrough may have quit.</p>
<p>Walkthrough is out of sync with the FMC:</p> <ul style="list-style-type: none"> <li>• Starts on the wrong step.</li> <li>• Advances prematurely.</li> <li>• Will not advance.</li> </ul>	<p>If a walkthrough is out of sync, you can:</p> <ul style="list-style-type: none"> <li>• Attempt to continue.</li> </ul> <p>For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task.</p> <ul style="list-style-type: none"> <li>• End the walkthrough, navigate to a different page, and try again.</li> </ul> <p>Sometimes you cannot continue. For example, if you do not click <b>Next</b> after you complete a step, you may need to end the walkthrough.</p>

## Sharing Data with Cisco

### Web Analytics tracking

In Version 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

You are enrolled in web analytics tracking by default (by accepting the Version 6.5.0+ EULA you consent to web analytics tracking), but you can change your enrollment at any time after you complete initial setup.



---

**Note** Upgrades to Version 6.2.3 through 6.6.x can enroll you in web analytics tracking. This can occur even if you purposely unenrolled. If you do not want Cisco to collect this data, unenroll after upgrading.

---

### **Cisco Success Network**

In Version 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

### **Cisco Support Diagnostics**

In Version 6.5.0+, *Cisco Support Diagnostics* (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.



---

**Note** This feature is supported on Firepower Management Centers and their managed Firepower Threat Defense devices. In Version 6.5.0 only, FTD support is restricted to the Firepower 4100/9300 with FTD and FTDv for Azure. This feature is not supported with Firepower Device Manager.

---

